security is not an island
HILTON MALTA

24th Annual FIRST Conference
MALTA
17 - 22 June 2012
Legal challenges to information sharing of national/governmental CERTs in Europe

Silvia Portesi
ENISA

Neil Robinson
RAND Europe
Agenda

• Importance of information sharing
• Policy background
• Information exchange: tensions with respect to the law
• 2011 ENISA study on information sharing of CERTs in Europe
• 2012 Good practice guide on legal aspects of CERTs and law enforcement cooperation
• Conclusions
Why does it help to share information?

- Cyber-attacks may cross organisational, national and public/private boundaries
- Mitigation requires concerted action and co-ordination which can be cross-border in nature
- Data provided by CERTs also helps to understand threats and trends

**Information sharing improves application of preventative measures and contributes to good cyber-security**
Policy background: an overview

- 2009 Digital Agenda for Europe (DAE)
  - Identifies that cyberspace now crucial for economic and social growth
- 2009 Communication on CIIP (COM 2009(149))
  - Indicates that Cybercrime or major forms of cyberattack might put economic and social benefits at risk
- 2011 Progress Report on CIIP (COM 2011(163))
  - Emphasises importance of national/governmental CERTs

Poor cybersecurity could threaten economic growth of Digital Europe – CERTs’ important role to prevent and handle incidents
Information exchange: tensions with respect to the law

- CERTs are acting to maintain or improve security
  - Unique role of national/governmental CERTs

- But in doing so they may have an impact on fundamental rights (e.g. right to protection of personal data)

- The uneven implementation of some EU law is also a challenge

- Uncertainty about what can and cannot be done might hinder CERTs in the performance of their role
2011 ENISA study on information sharing of CERTs in Europe

• Aim:
  • To support the operation and cooperation of (national/governmental) CERTs at a European level

• Some key questions:
  • Which are the relevant legal frameworks?
  • What legal and regulatory frameworks could pose a challenge?
  • What can we do to enhance the information exchange?
Our approach built logically from one stage to the next

- ENISA expertise
- External contractor (RAND Europe and time.lex)
- Input from the informal expert group
Several relevant legal frameworks identified

- Definitions of computer and network misuse
- Privacy and data protection legislation
- Public sector re-use of information
- Criminal procedure
- Intellectual property rights
- Determining applicable law
Cross border information exchange is not a rare event

- 58% never happened yet
- 16% more than once per month
- 16% six to twelve times per year
- 5% two to six times per year
- 5% less than twice per year

Conference Malta 17 - 22 June 2012
What legal reasons are used by CERTs declining to give information to other CERTs?

- Comptability with national law
- Comptability with internal rules
- The requesting party is unknown
- Legality of information request
- Mandate of the requesting party prohibits sharing
- Uncertainty about compatibility of request to requesters
What legal reasons do CERTs receive for not getting information from other CERTs?

- Comptability with national law
- Legality of information request
- Comptability with internal rules
- Organisation unknown to information owner
- Request incompatible with information owners own rules
- Mandate of your organisation prohibits sharing
- Requests never declined on legal grounds
An uncertain picture emerges

- CERTs exposed to cross border requests but lacking in legal expertise
- Data protection, data retention and laws relating to working with law enforcement were regarded as most relevant
- Less familiarity with international legal frameworks than national laws
- ‘Asymmetry’ of role of law in enabling information exchange
  - Reported as less problematic when preparing requests compared to responding to request from others
We derived some operational recommendations

• A.1: Establish direct approaches to support cooperation between CERTs
  • e.g. establishment of a centralised ‘legal hotline’
• A.2: Disseminate Declared Level of Service templates
• A.3: Investigative measures to encourage cross-border information exchange
  • e.g. exploring possibility of organisational models of sanitised sharing
  • e.g. exploring possibility of non-binding confidentiality charters and
And others aimed at addressing immediate policy issues

- B.1: Addressing legal uncertainty
- B.2: National/governmental CERTs on a specific legal footing
- B.3: EU-level legislation that takes account of scope of national/governmental CERTs
- B.4: Threshold for incidents requiring national/governmental CERTs response and sharing
- B.5: Articulate why CERTs need to process personal data to the relevant authorities
And finally longer-term recommendations

• C.1: Incorporate information on the legal basis for an information request

• C.2: Further foster R&D into privacy enhancing Security Event & Incident Monitoring (SEIM)

• C.3: Conduct further empirical research into cross-border CERT cooperation activities
A flair for sharing – encouraging information exchange between CERTs

A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe

Initial Edition 1.0
November 2011

http://www.enisa.europa.eu/activities/cert/support
Follow up ENISA activities in 2012

- Cybercrime projects 2012
  - Good practice guide on legal/regulatory aspects of cybercrime; and
  - Good practice guide on operational NIS aspects of the fight against cybercrime

- Both good practice guides are expected to be published by the end of the year on the ENISA website
2012 Good practice guide on legal aspects of CERTs & LEAs cooperation

Main goals:

- Describe the legal/regulatory aspects of the fight against cybercrime
- Compile an inventory of legal/regulatory and procedural challenges and possible ways to overcome these challenges
- Focus: Information exchange
  - between CERTs – Law enforcement agencies (LEAs) in Europe
  - between CERTs - CERTs/LEAs from Third Countries
- Collect existing good and best practices
- Develop recommendations
2012 Good practice guide on legal aspects - Informal Expert Group

- Composition
  - CERTs
  - Law Enforcement Agencies
  - Data Protection Authorities

- Discussion via email, teleconference and probably a F2F meeting

- Input during the development of the good practice guide and during the review process
2012 Good practice guide on legal aspects - Survey

- We are currently conducting an online survey to collect input for the 2012 good practice guide on legal aspects of CERTs and LEAs cooperation in the fight against cybercrime
- The survey is aimed at CERTs and also LEAs

Your input is important – please try to fill in the survey by 10th July 2012! The survey takes approximately 30 minutes to complete!
Conclusions

• Information sharing of CERTs and between CERTs & LEAs is paramount for the incident handling and for the fight against cyber crime
• A better understanding of the legal aspects helps to enhance the cross-boarder information sharing
• Addressing the (legal and operational) challenges of cross-border information sharing of CERTs and between CERTs and LEAs is an on-going process which requires joint efforts
Questions?
European Network and Information Security Agency (ENISA)
Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

cert-relations@enisa.europa.eu
silvia.portesi@enisa.europa.eu